

REMARKS

Claims 1-44 were pending at the time of the Office Action. Claims 8, 9, 20, 21, 32, 33, and 37-39 are cancelled in this response without prejudice. Claims 1-7, 10-19, 22-31, 34-36 and 40-44 are pending at this time. Claims 1, 13, 25, and 40 are independent claims. Claims 1-7, 10-19, 22-31, and 34-36 are amended. No new matter is added. Reconsideration and allowance of the above-referenced application are respectfully requested.

Claim Objections

Claim 4 is objected to for possible errors in the claim language. Amendments to claim 4 obviate the objection.

Claims 5, 8-10, 17, 20-22, and 32-34 are objected to due to improper claim dependencies. Claims 5, 10, 17, 22, and 34 are amended to overcome the objections. The cancellation of claims 8, 9, 20, 21, 32, and 33 obviate the rejections of these claims.

Accordingly, it is respectfully requested that the objections to the claims 4, 5, 10, 17, 22, and 34 be withdrawn.

35 USC 112

Claims 1, 2, and 37 stand rejected under 35 USC 112 as allegedly being indefinite. The amendments to claims 1 and 2 obviate the rejections. The cancellation of claim 37 obviates the rejection of claim 37.

The Office Action contends that there is no evidence in the claim language of the device being integrated into a secure network. Claim 1 is amended to recite, in part, "an authenticator in the network." Further, claim 1 recites, in part, "establishing an authenticated session between the device and the authenticator." Since an authenticated session is established between the device and the authenticator, and since

the authenticator is in the network, the claim clearly recites that the device is integrated into the secure network.

Further, the Office Action contends that it is unclear which entity is performing the hashing step and which entity is performing the comparing of the hashes and how the hashes are being sent to the network to enable a comparing step. See, e.g., Office Action, page 2, last paragraph - page 3, first paragraph. It is respectfully submitted that since claim 1 relates to a method claim, recitations of entities that perform the claimed subject matter are not required. Also, as amended, claim 1 is completely clear to one of ordinary skill in the art.

Furthermore, the Office Action contends that since the first and second secret are distinct items, it is confusing how a hash of two distinct strings of data would result in a positive match. See, e.g., Office Action, page 3, first paragraph. The amendments to the claims obviate these contentions. Further, claim 1 relates to generating a first hash using a secret obtained from a user, a first public key, a second public key, and a random number, and comparing the first hash with a second hash generated at a device. Claim 2 relates to generating the second hash using a second secret of the device, the first public key, the second public key, and the random number. If the second secret at the device matches the secret obtained from the user, then the first hash can match the second hash, since respective inputs to the first and second hashes will be the same.

At least for the above reasons, the rejection of claim 1 under 35 USC 112 should be withdrawn.

Claim 2 states, "generating the first hash at the device using the first public key, the second public key, the second secret, and the random number generated from the tunnel protocol." (Emphasis added). As amended, the random number

that is used to generate the hash of the second secret is the random number used to generate the hash of the first secret. Thus, the first hash can match the second hash if the secret obtained from the user is the same as the second secret. Accordingly, it is respectfully requested that the rejection of claim 2 under 35 USC 112 be withdrawn.

35 USC 103

Claims 1-5, 11-17, 23-29, and 35-44 stand rejected under 35 USC 103(a) as allegedly being unpatentable over Palekar et al. (US 2003/0226017), hereinafter "Palekar," in view of Peyravian et al. (US 20040158715), hereinafter "Peyravian." Claims 6-10, 18-22, and 30-34 stand rejected under 35 USC 103(a) as allegedly being unpatentable over Palekar in view of Peyravian and further in view of Slick et al. (US 2003/0105963), hereinafter "Slick." The rejections are respectfully traversed. The references, Palekar, Peyravian, and Slick, taken alone or in any combination, do not describe or suggest all the features of the claimed subject matter.

Palekar describes that an authentication protocol can be used to establish a secure method of communication between two devices on a network. Once established, the secure communication can be used to authenticate a client through various authentication methods. See, e.g., Palekar at Abstract. The Office Action contends that Palekar describes a device having a second secret and a second public key. See, Office Action, page 4, paragraph 4. This contention cannot be supported. Palekar does not describe or suggest a second secret and a second public key as claimed.

In this regard, Palekar states:

A secondary step of authentication mechanisms is proof of knowledge of the shared secret by the computing device seeking to be authenticated. Because generally no encryption mechanisms have yet been established between the two communicating endpoints, most authentication mechanisms avoid sending the shared secret itself, and instead rely on security devices such as a one-way hash. ... Alternatively, a key-hash can be used where the shared secret is the key used to hash an element of data. For example, the server computing device can send a random value to the client, and the client can key-hash the value using the client's password and return the hashed result to the server. The server can similarly key-hash the sent random value using the client's password, as stored in a database, on the server, and compare the results of the client's key-hash. (Emphasis added).

See, Palekar, [0044].

Thus, in Palekar, when a key-hash is used, the server sends a random value to the client, which the client key-hashes and returns to the server. Palekar does not describe or suggest that the client has a second secret and a second public key or that the server has a first public key. In addition, Palekar does not teach generating a first hash using a secret obtained from a user, the first public key, and the second public key, in addition to a random number. In contrast, claim 1 describes that a first hash is generated using a secret obtained from a user, the first public key, the second public key, and a random number. Therefore, Palekar does not describe or suggest the claimed subject matter.

Further, Palekar states:

The authenticating server can also respond with a certificate designed to authenticate the server to the client. Upon receipt of the server's response, the user's computing device can return its own certificate, designed to authenticate the client to the server and complete the mutual authentication, as

well as a client key exchange message, which either send the pre-master secret, or can send parameters from which the pre-master secret can be derived. The client can also indicate that the server's authentication was successful. When the server receives the client's certificate and the client key, it can verify the certificate and, if verified, signal to the client that its authentication was successful.

See, Palekar, [0048].

Thus, Palekar describes sending a certificate from the server to the client and another certificate from the client to the server to authenticate the server to the client and vice versa, respectively. The cited portions of Palekar (Palekar, [0044], lines 17-25, [0048]) do not describe or suggest generating a first hash using a secret obtained from a user, the first public key, the second public key, and a random number generated from the tunnel protocol, as claimed. Therefore, Palekar does not describe or suggest all the features of the claimed subject matter.

The Office Action contends that it would have been obvious to generate a hash using a first and second public key and a random number and asserts this to be a design choice. This contention is respectfully traversed. In this regard, the MPEP states:

In re Japikse, 181 F.2d 1019, 86 USPQ 70 (CCPA 1950) (Claims to a hydraulic power press which read on the prior art except with regard to the position of the starting switch were held unpatentable because shifting the position of the starting switch would not have modified the operation of the device.); *In re Kuhle*, 526 F.2d 553, 188 USPQ 7 (CCPA 1975) (the particular placement of a contact in a conductivity measuring device was held to be an obvious matter of design choice). However, "The mere fact that a worker in the art could rearrange the parts of the reference device to meet the terms of the claims on appeal is not by itself sufficient to support a finding of obviousness. The prior art must provide a motivation

or reason for the worker in the art, without the benefit of appellant's specification, to make the necessary changes in the reference device." *Ex parte Chicago Rawhide Mfg. Co.*, 223 USPQ 351, 353 (Bd. Pat. App. & Inter. 1984). (Emphasis added).

See, MPEP, 2144.04, VI, C.

It is respectfully submitted that generating the first hash, as claimed, is not accomplished by merely re-arranging known input parameters to a hashing function. Neither has the Office Action cited any reference that teaches generating a first hash using a secret obtained from a user, the first public key, the second public key, and a random number, as claimed, nor has the Office Action shown that one skilled in the art would be motivated to generate a first hash, as claimed. Therefore, the assertion that generating the first hash, as claimed, is a design choice is inappropriate.

Further, the Office Action contends that the prior art differs very little functionally only in that it requires the authenticator and device to maintain a shared secret, as opposed to 2 shared secrets (both public keys). See, Office Action, page 5, paragraph 1. This contention cannot be supported. As discussed previously, Palekar does not describe or suggest generating a first hash for transmission to the device, the first hash generated using a secret obtained from a user, the first public key, the second public key and a random number generated from the tunnel protocol. Therefore, the teachings of Palekar does not teach the features of the claimed subject matter.

Peyravian does not rectify these deficiencies in Palekar. Peyravian describes a method to exchange and authenticate public cryptographic keys between parties that share a common but secret password. See, Peyravian at Abstract. Peyravian states "...a client and a server know a common password a priori."

(Emphasis added). See, Peyravian, [0010]. Thus, in Peyravian, the common password is already known to both the client and the server before establishing any connection between the client and the server. Thus, in Peyravian, the server does not obtain the password from a user to generate a first hash because the server already possesses the secret. In contrast, as claimed, the second secret is obtained from a user for generating a first hash.

Since neither Palekar nor Peyravian, taken alone or in combination describe or suggest all the features of claim 1, a *prima facie* case of obviousness is not established. Accordingly, claim 1 is patentable. Claims 2-7 and 10-12 are also patentable at least for similar reasons and for the additional recitations that they contain.

Claim 13 is patentable at least for reasons similar to claim 1. Claims 14-19 and 22-24 are also patentable at least for similar reasons and for the additional recitations that they contain.

Claim 25 is patentable at least for reasons similar to claim 1. Claims 26-31 and 34-36 are also patentable at least for similar reasons and for the additional recitations that they contain.

Claim 40 is patentable at least for reasons similar to claim 1. Claims 41-44 are also patentable at least for similar reasons and for the additional recitations that they contain.

CONCLUSION

It is believed that all of the pending claims have been addressed. However, the absence of a reply to a specific rejection, issue or comment does not signify agreement with or concession of that rejection, issue or comment. In addition, because the arguments made above may not be exhaustive, there may be reasons for patentability of any or all pending claims

(or other claims) that have not been expressed. Finally, nothing in this paper should be construed as an intent to concede any issue with regard to any claim, except as specifically stated in this paper, and the amendment of any claim does not necessarily signify concession of unpatentability of the claim prior to its amendment.

In view of the foregoing amendments and remarks, Applicants respectfully submit that the application is in condition for allowance, and such action is respectfully requested at the Examiner's earliest convenience.

Please apply any credits or charges to deposit account 06-1050.

Respectfully submitted,

Date: _____

7/27/07



Scott C. Harris
Reg. No. 32,030
Attorney for Intel Corporation

Fish & Richardson P.C.
PTO Customer No.: 20985
12390 El Camino Real
San Diego, California 92130
(858) 678-5070 telephone
(858) 678-5099 facsimile

10740237.doc